

UNITED STATES DISTRICT COURT
for the
Northern District of New York

In the Matter of the Search of)
(Briefly describe the property to be searched)
or identify the person by name and address))
One (1) black colored Samsung Cellular)
Telephone, Model #: SM-S120VL(GP), FCC)
ID #: A3LSMS120VL, Serial #:)
GPSAS120VCB, IMEI #: 359259071509110,)
Made in Vietnam, with one (1) camouflage and)
black colored plastic case. SEE ALSO)
ATTACHMENTS A & B.)
)
)
)
)

Case No. 03:17-MJ- 368 (TWD)

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property:
(*identify the person or describe the property to be searched and its given location*):

SEE ATTACHMENT A. [This Search Warrant also seeks authorization to permit any forensic examiners who are assisting federal law enforcement officers to assist in and conduct execution of this Search Warrant and to conduct the forensic examination and analysis of items.]

located in the NORTHERN District of NEW YORK, there is now concealed
(*identify the person or describe the property to be seized*):
SEE ATTACHMENT B

The basis for the search under Fed. R. Crim. P. 41(c) is (*check one or more*):

- ☒ evidence of a crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

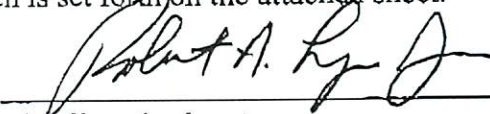
Code Section	Offense Description
--------------	---------------------

AO 106 (Rev. 04/10) Application for a Search Warrant (Page 2)

The application is based on these facts:
SEE ATTACHED AFFIDAVIT

☒ Continued on the attached sheet.

☐ Delayed notice of _____ days (give exact ending date if more than _____ Click here to enter a date.
is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.



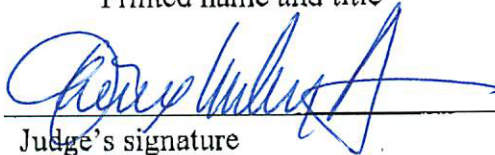
Applicant's signature

FBI Special Agent Robert A. Lyons, Jr.

Printed name and title

Sworn to before me and signed in my presence.

Date: August 24, 2017



Judge's signature

City and State: Syracuse, NY

Hon. Thérèse Wiley Dancks, U.S. Magistrate Judge

Printed name and title

ATTESTED TO BY THE APPLICANT IN ACCORDANCE WITH THE REQUIREMENTS OF RULE 4.1 OF
THE FEDERAL RULES OF CRIMINAL PROCEDURE.

**UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF NEW YORK**

**IN THE MATTER OF AN APPLICATION
OF THE UNITED STATES OF AMERICA
FOR SEARCH WARRANTS FOR:**

[SEE ATTACHMENTS A AND B, HEREIN]

3:17-mj-368

AFFIDAVIT IN SUPPORT OF APPLICATION FOR SEARCH WARRANT

ROBERT A. LYONS, JR., being duly sworn, deposes and states:

INTRODUCTION

1. I am a Special Agent of the United States Department of Justice, Federal Bureau of Investigation ("FBI"), and I am empowered by law to investigate and make arrests for offenses enumerated in Title 18, United States Code, Section 2516. As such, I am an "investigative or law enforcement officer" within the meaning of Title 18, United States Code, Section 2510(7).

2. I have been employed as a Special Agent of the FBI after having graduated from New Agents' Training at the FBI Academy in Quantico, Virginia in January 2013. I am currently assigned to the Albany Field Division, Binghamton Resident Agency, where I am responsible for conducting criminal investigations for violations of Title 18 and 21 of the United States Code to include controlled substances, criminal enterprises, street gangs, crimes against children, and other violent crimes. Prior to my employment with the FBI, I was employed as a Prosecutor's Detective with the Passaic County Prosecutor's Office located in Paterson, New Jersey for six years during which time I gained extensive training and investigative experience conducting criminal investigations into the physical neglect, sexual abuse, and sexual molestation of children under the age of eighteen.

3. I am currently investigating the production and distribution of an image constituting suspected child pornography of [REDACTED], DOB: XX/XX/2015, by Justin D. Crandall to [REDACTED], an associate of

Justin D. Crandall, that was uncovered during the course of an investigation conducted by the New York State Police, Troop C, Sidney Station, Bureau of Criminal Investigation.

4. During an interview with New York State Police personnel, [REDACTED] advised he had received the image of suspected child pornography (since identified as the minor female, [REDACTED]) and a series of sexually explicit text messages from Justin D. Crandall via a cellular telephone number connected to [REDACTED]'S Google Voice Account. [REDACTED] advised he used his Google Voice Account to communicate and share other nude images with Justin D. Crandall via his cellular telephone.

5. During the course of the sexual assault investigation conducted by the New York State Police, Troop C, Sidney Station, Bureau of Criminal Investigation, Investigators seized, among several other items, fourteen (14) electronic devices including cellular telephones, a laptop computer, several SD cards, and thumb drives from the residence of Justin D. Crandall, and his wife Jessica L. Crandall, located in Sidney, New York, during the execution of the New York State search warrant, as well as from the vehicle Justin D. Crandall operated on the night on February 11, 2017.

6. On February 16, 2017, the FBI, Albany Division, Binghamton Resident Agency, and the United States Attorney's Office for the Northern District of New York, opened a federal criminal investigation in connection with the captioned New York State Police investigation. During the course of the FBI investigation, your affiant obtained a federal search warrant on February 24, 2017 in order to search and seize the fourteen (14) electronic devices seized from the residence of Justin D. Crandall and his wife, Jessica L. Crandall, during the execution of the New York State search warrant, as well as from the vehicle Justin D. Crandall operated on the night of February 11, 2017.

7. On March 02, 2017, pursuant to the federal search warrant, Special Agent Stephen Vizvary of the Federal Bureau of Investigation, Albany Field Division, Binghamton Resident Agency, attempted to search a black colored Samsung Cellular Telephone, Model #: SM-S120VL(GP), FCC ID #: A3LSMS120VL, Serial #: GPSAS120VCB, IMEI #: 359259071509110, Made in Vietnam, with one (1) camouflage and black colored plastic case (hereafter, the "Subject Cellular Telephone", as more fully described in Attachment A) seized from the vehicle Justin D. Crandall operated on the night of February

11, 2017. In doing so, Special Agent Vizvary determined the Subject Cellular Telephone was password protected and he was not able to extract all the data or all other contents stored within the Subject Cellular Telephone. However, Special Agent Vizvary located a 16GB Micro SD card inserted in a media slot within the housing of the Subject Cellular Telephone and was able to extract several images and video files constituting the sexual exploitation of [REDACTED]

8. Additionally, Special Agent Vizvary employed an alternative method to bypass and defeat the password lock on the Subject Cellular Telephone. Special Agent Vizvary conducted a file system extraction¹ of the Subject Cellular Telephone using a commercial software package available to law enforcement agencies known as Universal Forensic Extraction Device (UFED)². In reviewing the results of the file system extraction of the Subject Cellular Telephone, Special Agent Vizvary advised that the file system extraction bypassed the password lock which gained access to a small portion of the Subject Cellular Telephone's file structure but only extracted a limited portion of the data and other files stored within the Subject Cellular Telephone. However, embedded within the extracted data and files, Special Agent Vizvary and your affiant located several different video files constituting the sexual exploitation of [REDACTED], not previously identified on or extracted from the 16GB Miro SD card inserted in a media slot within the housing of the Subject Cellular Telephone. Although this data was extracted, no chat logs, text messages, multimedia messages, Internet browsing history, downloaded and installed applications, e-mail messages, other file folders, etc. were extracted from the Subject Cellular Telephone. As a result, it appears to your affiant the Subject Cellular Telephone may contain additional images, video files, text messages, e-mail messages, downloaded applications, and other information relative to the physical and sexual exploitation of [REDACTED] by Justin D. Crandall and Jessica L. Crandall. Based upon the information contained in this affidavit, your affiant requests this Court issue the attached search warrant and application authorizing the FBI to utilize different techniques not already tried or attempted in order

¹ A file system extraction is the acquisition of the files embedded in the memory of a cellular telephone or mobile device. Performing a file system extraction provides access to all of the files present in the cellular telephone or mobile device's memory at the time of the extraction.

² Universal Forensic Extraction Device (UFED) is a software package manufactured by Cellebrite that allows law enforcement and other governmental agencies to extract data and files from mobile devices.

to search the Subject Cellular Telephone for the items more particularly described in Attachment B. The FBI currently has reason to believe that a current technique(s) exist that will allow for extraction of password protected data and files from the Subject Cellular Telephone which were not able to be extracted during the previous search. For that reason application is made for this search warrant.

9. As will be demonstrated in this affidavit, there is probable cause to believe that evidence will be located on the Subject Cellular Telephone relating to violations of Title 18, United States Code, Sections 2251 (sexual exploitation of children, and the attempt and conspiracy to commit that offense), and 2252/2252A (receipt, distribution, and/or possession of child pornography, and the attempt to commit said offenses): (hereafter referred to as the "Subject Offenses"). I submit this affidavit in support of a search warrant and application authorizing the FBI and law enforcement to utilize different techniques not already tried or attempted in order to search of the Subject Cellular Telephone for evidence of those particular crimes, as further described in Attachment B including evidence, fruits, and instrumentalities of the Subject Offenses, as well as additional evidence of those offenses including additional images of [REDACTED], sexually explicit text messages between Justin D. Crandall and [REDACTED]; other information relative to the physical and sexual exploitation of [REDACTED] by Justin D. Crandall and Jessica L. Crandall including photographs, video files, text messages; inappropriate or otherwise illegal images and video files of Justin D. Crandall and Jessica L. Crandall's [REDACTED] and other identifying information to confirm the user and operator of the Subject Cellular Telephone.

10. I request authority from the United States District Court, Northern District of New York, for the FBI to search the Subject Cellular Telephone wherein the items specified in Attachment B may be found, and to seize any and all items listed in Attachment B as instrumentalities, fruits, and evidence of associated criminal activities and the Subject Offenses. The Subject Cellular Telephone is currently in the custody of the FBI and stored at the Office of the FBI, Albany Field Division, Syracuse Resident Agency, business address 250 South Clinton Street, Syracuse, New York 13202.

11. The statements and facts set forth in this affidavit are based in significant part on: my review of written documents and the audio/video recorded interviews of Justin D. Crandall and Jessica L.

Crandall conducted by the New York State Police; my review of images and video files extracted from a 16GB Miro SD card contained within the Subject Cellular Telephone as well as other video files extracted from file system extraction of the Subject Cellular Telephone; my conversations with other members of the FBI and the New York State Police; and my own investigation into this matter. Since this affidavit is being submitted for the limited purposes of securing a search warrant, I have not included each and every fact known to me concerning this ongoing investigation. I have set forth only the facts and circumstances that I believe are necessary to establish probable cause to believe that evidence, fruits, and instrumentalities of the violations of Title 18, United States Code, Sections 2251, 2252 and 2252A are presently located on the Subject Cellular Telephone.

STATUTORY AUTHORITY

12. This investigation concerns alleged violations of Title 18, United States Code, Sections 2251, 2252, and 2252A, relating the sexual exploitation of minors:

- a. 18 U.S.C. § 2251(a) prohibits employing, using, persuading, inducing, enticing, or coercing and minor to engage in any sexually explicit conduct for the purpose of producing any visual depiction of such conduct or for the purpose of transmitting a live visual depiction of such conduct, if such person knows or has reason to know that such visual depiction will be transported or transmitted using any means or facility of interstate or foreign commerce or in or affecting such commerce or mailed, or that visual depiction was produced or transmitted using materials that have been mailed, shipped, or transported in or affecting interstate or foreign commerce by any means, or if such visual depiction has actually been transported or transmitted using any facility of interstate or foreign commerce or in or affecting interstate or foreign commerce or mailed. Section 2251(e) makes it a violation to conspire or attempt to commit this offense.

- b. 18 U.S.C. § 2252(a)(1) prohibits knowingly transporting or shipping in interstate or foreign commerce, by computer or mail, any visual depiction of minors engaging in sexually explicit conduct.
- c. 18 U.S.C. § 2252(a)(2) prohibits knowingly receiving or distributing, by computer or mail, any visual depiction of minors engaging in sexually explicit conduct that has been mailed, shipped, or transported in interstate or foreign commerce. That section also prohibits knowingly reproducing any visual depiction of minors engaging in sexually explicit conduct for distribution in interstate or foreign commerce by any means, including by computer or the mail.
- d. 18 U.S.C. § 2252(a)(4) prohibits possessing one or more books, magazines, periodicals, films, or other materials which contain visual depictions of minors engaged in sexually explicit conduct that have been transported in interstate or foreign commerce, or that were produced using materials that had traveled in interstate or foreign commerce.
- e. 18 U.S.C. §§ 2252(b)(1) and (2) make it a violation to attempt to commit any of the above offenses.
- f. 18 U.S.C. § 2252A(a)(1) prohibits knowingly mailing, transporting, or shipping child pornography in interstate or foreign commerce by any means.
- g. 18 U.S.C. § 2252A(a)(2) prohibits knowingly receiving or distributing any child pornography that has been mailed or shipped or transported in interstate or foreign commerce by any means, including by computer.
- h. 18 U.S.C. § 2252A(a)(3)(A) prohibits a person from knowingly reproducing child pornography for distribution through the mail or in interstate or foreign commerce by any means, including by computer.
- i. 18 U.S.C. § 2252A(a)(3)(B) prohibits knowingly advertising, promoting, presenting, distributing, or soliciting through the mail, or using any means or

facility of interstate or foreign commerce, or in or affecting interstate or foreign commerce by any means any material in a manner that reflects the belief or is intended to cause another to believe that the material is or contains a visual depiction of an actual minor engaging in sexually explicit conduct, or an obscene visual depiction of a minor engaging in sexually explicit conduct.

- j. 18 U.S.C. § 2252A(a)(5)(B) prohibits a person from knowingly possessing any book, magazine, film, videotape, computer disk, or other material that contains an image of child pornography that has been mailed, shipped, or transported in interstate or foreign commerce by any means, including by computer, or that was produced using materials that have been mailed, shipped, or transported in interstate or foreign commerce by any means, including by computer.
- k. 18 U.S.C. §§ 2252A(b)(1) and (2) make it a violation to attempt to commit any of the above offenses.

DEFINITIONS

- 13. The following definitions apply to this affidavit and Attachment D:
 - a. “Child Erotica” means materials or other items that are sexually arousing to persons having a sexual interest or desire in minors but that are not necessarily, in and of themselves, obscene or that do not necessarily depict minors in sexually explicit poses or body positions.
 - b. “Child Pornography” includes any visual depiction of sexually explicit conduct where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct; (b) the visual depiction was a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct; or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct. See 18 U.S.C. § 2256(8).

- c. “Computer” refers to “an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device.” See 18 U.S.C. § 1030(e)(1).
- d. “Computer-related documentation” consists of written, recorded, printed, or electronically stored material that explains or illustrates how to configure or use computer hardware, computer software, or other related items.
- e. “Computer software” is digital information that can be interpreted by a computer and any of its related components to direct the way it works. Computer software is stored in electronic, magnetic, or other digital form. It commonly includes programs to run operating systems, applications, and utilities.
- f. “Computer hardware,” as used herein, consists of all equipment which can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data-processing devices (including, but not limited to, central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, floppy disk drives and diskettes, and other memory storage devices); peripheral input/output devices (including, but not limited to, keyboards, printers, video display monitors, and related communications devices such as cables and connections), as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware.
- g. “Minor” means any person under the age of 18 years. See 18 U.S.C. § 2256(1).
- h. “Sexually explicit conduct” applies to the visual depictions that involve the use of a minor, see 18 U.S.C. § 2256(8)(A), or that have been created, adapted, or modified to appear to depict an identifiable minor, see 18 U.S.C. § 2256(8)(C). In those contexts, the term refers to actual or simulated: (a) sexual intercourse

(including genital-genital, oral-genital, or oral-anal), whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the genitals or pubic areas of any person. See 18 U.S.C. § 2256(2)(A).

- i. “Visual depictions” include undeveloped film and videotape, as well as data stored on computer disk or by electronic means, which is capable of conversion into a visual image. See 18 U.S.C. § 2256(5).

BACKGROUND ON COMPUTERS AND CHILD PORNOGRAPHY

14. Based on my knowledge, training, and experience, and the experience and training of other law enforcement agents and investigators with whom I have had discussions, cellular telephones, computers, computer technology, and the Internet have completely revolutionized the manner in which child pornography is possessed, received, produced and distributed.

15. Computers, storage devices, and cellular telephones serve four different roles or functions with child pornography: production, communication, distribution, and storage.

16. The computer’s and cellular telephone’s ability to store images in digital form makes the computer and cellular telephone itself an ideal repository for child pornography. The size of the electronic storage media (commonly referred to as the hard drive or the memory) used in computers and cellular telephones has grown tremendously within the last several years. These hard drives and memory can store literally thousands of images at very high resolution.

17. As with most digital technology, communications made from a computer or a cellular telephone are often saved or stored on that computer’s hard drive or cellular telephone. Storing this information can be intentional, for example, by saving an e-mail as a file on the computer or cellular telephone, or saving the location of a favorite website in “bookmarked” files. Digital information, however, can also be retained unintentionally. Traces of the path of an electronic communication may be automatically stored in many places, such as temporary files or ISP client software, among others. In addition to electronic communications, a cellular telephone or computer user’s Internet activities

generally leave traces in a cellular telephone or computer's web cache and Internet browsing history files. A trained digital forensic examiner often can recover evidence and other items that show whether a computer or cellular telephone contains peer-to-peer software, when the cellular telephone or computer was sharing data files, and some of the data files that were uploaded, downloaded and transferred. Such information is often maintained indefinitely until overwritten by other data.

18. Modern technology in the past several years has transformed the cellular telephone from a simple mobile telephone device into a mobile mini-computer commonly referred to as a "smart phone" capable of Internet access through wireless internet connections as well as cellular telephone signals; built in digital camera and video camera capabilities are common features; video and image storage capabilities can hold thousands of images and hours of video files; and by being able to access the Internet virtually anywhere, digital images and videos taken with a cellular telephone and stored on the cellular telephone can be shared with others by e-mail (phone to computer), text messaging (phone to phone), and uploaded to and displayed on Internet websites. Smart phones generally have global positioning satellite (GPS) capabilities that allow the cellular telephone to provide driving directions, and include GPS coordinates in such features as sharing locations on social networking websites and imbedding into the metadata of photographic images the coordinates of where an image was taken.

19. Collectors and distributors of child pornography also use online resources to retrieve and store child pornography including services offered by Internet Portals such as Yahoo! and Hotmail, among others. These online services allow a user to set up an account with a remote computing service that provides e-mail services as well as the electronic storage of computer files in any variety of formats. A user can set up an online storage account from any computer or cellular telephone with access to the Internet. Evidence of such online storage of child pornography is often found on the user's cellular telephone and computer's hard drive. Even in cases where online storage is used, evidence of child pornography can be found on the user's cellular telephone or computer in most cases.

COLLECTORS OF CHILD PORNOGRAPHY

20. Individuals who are interested in child pornography may want to keep the child

pornography files they create or receive for additional viewing in the future. Individuals who collect child pornography may go to great lengths to conceal and protect from discovery their collections of illicit materials. They often maintain their collections in the privacy of their homes, on computers, on external hard drives, on cellular telephones, or in other secure locations:

21. Individuals who collect child pornography may search for and seek out other like-minded individuals, either in person or on the Internet, to share information and trade depictions of child pornography and child erotica as a means of gaining status, trust, acceptance and support. This contact also may help these individuals to rationalize and validate their deviant sexual interest and associated behavior. The different Internet-based vehicles used by such individuals to communicate with each other include, but are not limited to: text messages, video messages, electronic mail, email, bulletin boards, IRC, chat rooms, newsgroups, instant messaging, and other vehicles.

22. Individuals who collect child pornography may keep names, electronic mail addresses, cellular and telephone numbers or lists of persons who have shared, advertised, or otherwise made known their interest in child pornography or sexual activity with children. These contacts may be maintained as a means of personal referral, exchange, and/or commercial profit. This information may be maintained in the original medium from which it was derived.

BACKGROUND OF THE INVESTIGATION

23. On February 11, 2017, the New York State Police received a complaint from [REDACTED] (the Complainant) in which he reported he had received an image of a minor child engaged in a sexual act via the Google Voice Text Messaging Service on either February 8, 2017 or February 9, 2017. Briefly and in part, [REDACTED] advised he received this image from an old acquaintance named Justin D. Crandall from a Verizon Wireless Account. [REDACTED] described the image as an erect male's uncircumcised penis resting on the face of a minor female in which the minor female's hand was holding the male's penis. [REDACTED] advised he believed the erect male's uncircumcised penis depicted in the image was Justin D. Crandall's penis since he and Justin D. Crandall had exchanged several naked images of themselves from the waist down over the last two years. Although the image quality was poor and dark, [REDACTED] advised that he did not

recognize the minor female depicted in the image. [REDACTED] opined the minor female depicted in the image had blonde hair and was between the ages of 3 and 8.

23a. After receiving this image from Justin D. Crandall, [REDACTED] advised he became concerned for the safety of the minor female depicted in the image. [REDACTED] advised he recalled having text message conversations with Justin D. Crandall in January 2017 during which Justin D. Crandall declared he had a "little whore" he was in the process of training. During these conversations, Justin D. Crandall advised [REDACTED] that his wife babysat for the "little whore." Justin D. Crandall informed [REDACTED] he was trying to get "her" to open her mouth and have oral sexual contact with Justin D. Crandall's penis. Justin D. Crandall also described how he ejaculated on "her" face and attempted vaginal sexual intercourse on "her." However, Justin D. Crandall reported "she" was too tight to allow him to insert his penis all the way into "her" vagina, but he inserted the head of his penis into "her" vagina and ejaculate.

23b. Besides these sexual activities, Justin D. Crandall advised [REDACTED] that he was trying to "whore her out." At that time, Justin D. Crandall asked [REDACTED] to locate a "creepy old man who might be into that kind of thing and has a bunch of money." [REDACTED] advised that he was not sure who "her" and "she" was throughout these text message conversations. At first, [REDACTED] advised that he believed Justin D. Crandall was describing a sexual fantasy or an old ex-girlfriend who was willing to engage in the aforementioned described sexual activities. However, after observing the image Justin D. Crandall sent to [REDACTED] of the minor female, [REDACTED] now believed Justin D. Crandall was describing the minor female depicted in the image throughout the entirety of their conversation in January 2017.

23c. Following the interview with [REDACTED] [REDACTED] provided the New York State Police written consent to conduct a search of his computer. [REDACTED] advised that the text messaging conversations and the image of the minor female sent by Justin D. Crandall were still preserved within the Google Voice Account stored on his computer. After obtaining written consent, members of the New York State Police reviewed these text messaging conversations within the Google Voice Account, as well as the image of the minor female as described by [REDACTED] during his interview. The New York State Police were able to confirm the content and nature of the text message conversations between [REDACTED] and Justin D. Crandall as

well as the image of the minor child sent by Justin D. Crandall. The New York State Police documented these text messages and the image of the minor child with digital photography before seizing the [REDACTED] computer for additional forensic extraction and analysis.

24. On February 14, 2017 the New York State Police provided to your affiant one compact disc (CD) containing digital images of the sexually explicit text message conversations and the image of the minor child sent by Justin D. Crandall. After reviewing some of the sexually explicit text message conversations containing on the CD as well as through a federal search warrant served on Google, Inc. by your affiant on February 24, 2017, your affiant also confirmed the content and nature of the sexually explicit text message conversations between [REDACTED] and Justin D. Crandall as described by [REDACTED] and the image of the minor child sent by Justin D. Crandall to [REDACTED]. These items are available for the Court's review upon request. Below are some verbatim excerpts of the sexually explicit text messages sent by Justin D. Crandall using his Verizon Wireless Account to [REDACTED] as preserved by the New York State Police in [REDACTED] Google Voice Account on February 11, 2017 and returned from Google, Inc. pursuant to the federal search warrant served on February 24, 2017:

- 24a. Sent from Justin Crandall (mobile) – Jan 11, 10:49 PM: “My woman baby sits an I would never harm my kids so it has nothin to do with them but it has to do with the little Whore& in training she watch’s”
- 24b. Sent from Justin Crandall (mobile) – Jan 11, 11:00 PM: “Really the only thing shes good for right now is dick smacking tryin to get her to open her mouth so u can attempt to get a bj spit in her face. Smack her throw her around. Jus can’t leave bruises. Scare the fuck out of her. Deff cum on her face an rub it all around. Feed it to her but the stupid cunt doesn’t do anything. She’s got one of these faces u wish cud blacken. Sit on her face even. Ahe made this girl my age cum the otherday I pushed her head into my friends pussy an cry in made her cum all over”

24c. Sent from Justin Crandall (mobile) – Jan 11, 11:09 PM: “But if u pull ur dick out so ur balls are on her chin ur dick will go past her forehead. The otherday she made me cum literally alday I rubed the tip of my sick all over her wet spit face esp her nose an dumped like 5 loads on her that day but like I said shes in training by time I get done with her she’s gonna be eatin loads off the floor. Least now when u pull ur dick out to her mouth she goes in and touch’s her lips with it”

25. After speaking with [REDACTED] on February 11, 2017, the New York State Police applied for and obtained a search warrant to search Justin D. Crandall and Jessica L. Crandall’s residence located in Sidney, New York. During the execution of this search warrant on the residence, the New York State Police seized fourteen (14) electronic devices from the residence of Justin D. Crandall, and his wife, Jessica L. Crandall, among several other physical items.³

26. While the search warrant was being executed, the New York State Police located Justin D. Crandall standing next to his vehicle close to his residence on Bird Avenue in Sidney, New York. After being contacted by the New York State Police, Justin D. Crandall voluntarily agreed to be interviewed and was transported by members of the New York State Police to New York State Police, Sidney Station, located in Sidney, New York. Prior to transporting Justin D. Crandall, a New York State Police Investigator observed the Subject Cellular Telephone inside the Justin D. Crandall’s vehicle in plain view. After confirming with Justin D. Crandall that the Subject Cellular Telephone was in fact Justin D. Crandall’s personal cellular telephone, the New York State Police Investigator seized the Subject Cellular Telephone from inside Justin D. Crandall’s vehicle. Believing that the Subject Cellular Telephone was used to take the sexually explicit image of [REDACTED] sent to [REDACTED] and thus may contain evidence of that photograph as well as being cognizant of the fact individuals can wipe the contents or

³ Since the acquisition of the New York state search warrant, the New York State Police never searched these items. Since then, the FBI and the United States Attorney’s Office for the Northern District of New York have opened a federal criminal investigation into this matter. In a previous affidavit and application dated February 24, 2017, your affiant requested federal search and seizure warrants for these fourteen (14) electronic devices and [REDACTED] computer given that they were now in FBI custody. In addition, search and seizure warrants were requested for the Verizon Wireless account accessed by Justin D. Crandall and the Google Voice Account accessed by [REDACTED]

data of their cellular telephone remotely and without physical access to the cellular telephone, the New York State Police Investigator seized the Subject Cellular Telephone to prevent the destruction of evidence pending the acquisition of a separate New York State search warrant to actually forensically search the Subject Cellular Telephone at a later date and time⁴.

27. After arriving at the New York State Police, Sidney Station, and after being advised of his Miranda Rights, Justin D. Crandall voluntarily provided the following information:

27a. Initially, Justin D. Crandall denied knowing why he was being interviewed at the New York State Police, Sidney Station, and denied sending any images constituting child pornography via text message to any of his friends or close associates.

27b. However, during the course of the interview, Justin D. Crandall advised that he recently took and sent the image of his erect penis resting on the face of his neighbor's minor female child via text message. Justin D. Crandall confirmed the minor female child's hand was touching his erect penis in the image he sent. Although Justin D. Crandall claimed he did not know the name of the minor female child depicted in the image, Justin D. Crandall advised the minor female child's mother was named [REDACTED] and they lived [REDACTED] and his family on [REDACTED]. Justin D. Crandall advised that his cellular telephone, identified as a Samsung cellular telephone which is the Subject Cellular Telephone, contained three images of the minor female child. In addition, Justin D. Crandall reported the Subject Cellular Telephone may contain other images of [REDACTED] images he said he took because his [REDACTED] was gaining weight.

27c. Justin D. Crandall also advised that since he began consuming the controlled substance methamphetamine on a regular basis his days were somewhat blurry and his sexual drive had apparently kicked into a whole new level. Justin D. Crandall admitted he touched the minor female child in a sexual manner when he was under the influence of methamphetamine. Specifically, when asked if he had engaged in "sex" with the minor female child, Justin D. Crandall asked investigators to define the term

⁴ The New York State Police Investigator did obtain a separate New York State search warrant; however, the New York State Police did not search the Subject Cellular Telephone. Instead, the FBI obtained a federal search and seizure warrant to search the Subject Cellular Telephone on February 24, 2017.

“sex.” When the New York State Police provided him with a definition, Justin D. Crandall denied placing his penis inside of the minor female child’s mouth or vagina and ejaculating on the minor female child, but instead advised he placed his penis on the top of the minor female child’s vaginal area.

28. Following the interview of Justin D. Crandall, the New York State Police arrested Justin D. Crandall and charged him with Rape in the First Degree in violation of New York State Penal Code, Section 130.35, among other New York State criminal violations. Following his arraignment, Justin D. Crandall was remanded to the Delaware County Jail in Delhi, New York.

29. On February 12, 2017, the New York State Police interviewed [REDACTED] the mother of [REDACTED] a 17 month old female child at that time, at the New York State Police, Sidney Station, in Sidney, New York. Briefly and in part [REDACTED] advised Jessica L. Crandall and Justin D. Crandall began [REDACTED] on Monday evenings after the Thanksgiving holiday in late November 2016.

29a. Recently [REDACTED] advised she noticed some changes in [REDACTED] behavior. [REDACTED] advised [REDACTED] tended to cling more to [REDACTED] when [REDACTED] dropped [REDACTED] at Jessica L. Crandall’s residence, especially when Justin D. Crandall was present. In addition [REDACTED] recently noticed an unexplained mark, similar to a scratch, on [REDACTED] right check and a bite mark on her left arm. When [REDACTED] picked [REDACTED] from Jessica L. Crandall’s residence, [REDACTED] noticed the injuries as well as concealing makeup applied on [REDACTED] face. [REDACTED] asked Jessica L. Crandall what had occurred and in response, Jessica L. Crandall simply advised her son had bit [REDACTED] in the arm and threw something at [REDACTED] face.

29b. In addition to these injuries, [REDACTED] advised she uncovered several other bruises or marks on [REDACTED] body in places such as her head, the upper thigh of her right leg, her left upper thigh, and her butt. [REDACTED] advised she was extremely upset and immediately contacted Jessica L. Crandall. [REDACTED] advised Jessica L. Crandall’s tone was very defensive and that she informed [REDACTED] she treated [REDACTED] as one of her own children. [REDACTED] initially backed off from questioning Jessica L. Crandall any further about these injuries and marks on [REDACTED]. However, [REDACTED] began to question whether Jessica L. Crandall and Justin D. Crandall should continue to [REDACTED] moving forward in the future.

29c. Lastly, in the past couple of days, [REDACTED] advised [REDACTED] had been wetting her diapers at a greater frequency and had showed some defiance and discomfort when trying to wipe [REDACTED] vaginal and anal areas. [REDACTED] advised [REDACTED] now tightly clenched her legs together when she produced fecal matter making it extremely difficult to sufficiently clean [REDACTED] anal area. [REDACTED] sensed it was almost as if [REDACTED] did not want anyone touching her private areas at all.

30. On February 13, 2017, Jessica L. Crandall was contacted by the New York State Police and agreed to be interviewed at the New York State Police, Sidney Station, located in Sidney, New York, in connection with the investigation. After being advised of her Miranda Warnings and Rights, Jessica L. Crandall voluntarily provided the following information:

30a. Beginning in or around December 2016, Jessica L. Crandall advised Justin D. Crandall and her engaged in repeated sexual activities with [REDACTED] minor female child, [REDACTED] a minor child under the age of 2, while Jessica L. Crandall and Justin D. Crandall [REDACTED] at their residence located in Sidney, New York. Jessica L. Crandall advised the sexual abuse of [REDACTED] began when Justin D. Crandall attempted to place his penis into [REDACTED] mouth.

30b. On January 02, 2017, Jessica L. Crandall advised that Justin D. Crandall attempted to place his penis in [REDACTED] mouth and then spat on her. Since he could not insert his penis into [REDACTED] mouth, Justin D. Crandall attempted to place his penis inside [REDACTED] vagina after he spat on his erect penis as well as [REDACTED] vagina for lubrication. Jessica L. Crandall advised Justin D. Crandall was unable to place his penis inside of [REDACTED] vagina because [REDACTED] was clenching her legs in discomfort. Jessica L. Crandall advised she masturbated herself and watched Justin D. Crandall while he attempted to place his penis inside of [REDACTED] vagina. Jessica L. Crandall then advised she watched Justin D. Crandall as he masturbated and ejaculated on [REDACTED] stomach.

30c. On January 23, 2017, Jessica L. Crandall advised that Justin D. Crandall bound her legs with a sheet and her hands with Velcro straps from his toolbox. Jessica L. Crandall advised Justin D. Crandall also bound [REDACTED] arms in the same fashion with Velcro on the other side of their bed. Jessica L. Crandall advised that she performed oral sexual contact on Justin D. Crandall while he moved back and

forth between [REDACTED] and Jessica L. Crandall. When Justin D. Crandall moved toward [REDACTED] position on the bed, Jessica L. Crandall advised Justin D. Crandall struck [REDACTED] in the head with his erect penis on approximately three separate occasions before he told Jessica L. Crandall to suck on his erect penis until he climaxed. After being untied, Jessica L. Crandall went into the bathroom to clean herself up at Justin D. Crandall's request. A short time later, Justin D. Crandall entered the bathroom carrying [REDACTED] and then placed [REDACTED] in the bathtub. Justin D. Crandall then ordered Jessica L. Crandall to clean up [REDACTED] so Jessica L. Crandall gave [REDACTED] a bath. It should be noted a state search warrant executed on Justin D. Crandall and Jessica L. Crandall's residence by the New York State Police recovered the aforementioned Velcro straps believed to have been used by Justin D. Crandall during this incident.

30d. On February 06, 2017, Jessica L. Crandall advised she observed a flea or bug in [REDACTED] hair so she placed mayonnaise in [REDACTED] hair as a home remedy. Jessica L. Crandall then advised Justin D. Crandall took a spoonful of mayonnaise and threw it on [REDACTED] and directed Jessica L. Crandall to rub mayonnaise over [REDACTED] body. While Jessica L. Crandall was rubbing the mayonnaise on [REDACTED] body, Jessica L. Crandall advised she observed Justin D. Crandall rubbing his penis over his clothes. Jessica L. Crandall believed Justin D. Crandall was sexually aroused while watching Jessica L. Crandall place mayonnaise on [REDACTED] body. Jessica L. Crandall observed Justin D. Crandall take a digital photograph of [REDACTED] covered in mayonnaise with his cellular telephone, believed to be the Subject Cellular Telephone in Attachment A. Although [REDACTED] did not have a shirt on covering her upper body, Jessica L. Crandall advised [REDACTED] did have a diaper on that covered her private areas.

30e. Also on February 06, 2017, Justin D. Crandall performed oral sexual contact on Jessica L. Crandall and then placed [REDACTED] head in her (Jessica L. Crandall) vaginal area for a period of approximately thirty seconds to one minute. Jessica L. Crandall advised she felt [REDACTED] nose touch her buttocks as Justin D. Crandall pushed [REDACTED] face into Jessica L. Crandall's vaginal area. Jessica L. Crandall advised while [REDACTED] head was in her vaginal area, Justin D. Crandall informed her to look up and say "cheese" as he took a digital photograph using his cellular telephone, believed to be the Subject Cellular Telephone, while [REDACTED] was situated in between Jessica L. Crandall's spread legs.

30f. Jessica L. Crandall advised she knew the child sexual abuse of [REDACTED] was wrong. In mitigation, Jessica L. Crandall advised she tried not to orgasm during the sexual activities involving [REDACTED] and Justin D. Crandall. Jessica L. Crandall allowed the child sexual abuse to occur simply because Justin D. Crandall paid more sexual attention to her when [REDACTED] was involved.

30g. In addition to the sexual abuse of [REDACTED], Jessica L. Crandall advised Justin D. Crandall also engaged in physical abuse on some occasions. During the first occasion, Jessica L. Crandall advised Justin D. Crandall bit [REDACTED] when she would not stop crying. On the second occasion, Justin D. Crandall pushed [REDACTED] and she hit her chin on a stand in the bedroom of their residence. Jessica L. Crandall advised [REDACTED] developed a small bruise on her face. Jessica L. Crandall advised Justin D. Crandall requested Jessica L. Crandall take care of the bruise. As a result, Jessica L. Crandall placed cosmetic makeup on [REDACTED] face in order to conceal the extent of the injury. Jessica L. Crandall and Justin D. Crandall were concerned [REDACTED] mother would locate the injury and ask questions.

31. Following the interview of Jessica L. Crandall, the New York State Police arrested Jessica L. Crandall and charged her with Criminal Sexual Act in the First Degree in violation of New York State Penal Code, Section 130.50, and Endangering the Welfare of a Child in violation of New York State Penal Code, Section 260.10. Following her arraignment, Jessica L. Crandall was remanded to the Delaware County Jail located in Delhi, New York.

32. On February 16, 2017, the FBI, Albany Division, Binghamton Resident Agency, and the United States Attorney's Office for the Northern District of New York, opened a federal criminal investigation in connection with the captioned investigation.

33. On February 16, 2017, the FBI and the United States Attorney's Office for the Northern District of New York charged Justin D. Crandall and Jessica L. Crandall via a federal felony complaint with one count each of Title 18, United States Code, Section 2251(a)&(e) [Conspiracy to Sexually Exploit a Child], and one count each of Title 18, United States Code, Section 2251(a)&(e), and 2 [Sexual Exploitation of a Child]. Both Justin D. Crandall and Jessica L. Crandall were arrested by the FBI on February 17, 2017. Following their Initial Appearance in United States District Court, Northern District

of New York on February 17, 2017, they were remanded into the custody of the United States Marshal Service and transported to the Delaware County, New York jail.

34. On March 02, 2017, pursuant to the federal search warrant dated February 24, 2017, Special Agent Stephen Vizvary of the Federal Bureau of Investigation, Albany Field Division, Binghamton Resident Agency, attempted to search the Subject Cellular Telephone seized from the vehicle Justin D. Crandall operated on the night of February 11, 2017. In doing so, Special Agent Vizvary observed the Subject Cellular Telephone was password protected and he was not able to extract all the data or all other contents stored within the Subject Cellular Telephone. However, Special Agent Vizvary located a 16GB Micro SD card inserted in a media slot within the housing of the Subject Cellular Telephone and he was able to extract several images and video files constituting the sexual exploitation of [REDACTED] in a folder entitled, "My cum dump," and other folders. A sample of these images and video files, which are available for the Court's review upon request, are described below as follows:

- "20170116_225802.jpg": This image file depicts an uncircumcised penis being held by a human hand and placed on the mouth of [REDACTED]
- "20170130_215330.jpg": This image depicts [REDACTED] without a shirt on and standing tall with a dark colored strap over her mouth, her hands bound behind her back with a dark colored strap, and her feet bound together with another dark colored strap.
- "20170207_104408.jpg": This image depicts [REDACTED] mouth kissing Justin D. Crandall's exposed uncircumcised penis during which Justin D. Crandall's face is partially visible.
- "20170207_104417.jpg": This image depicts [REDACTED] mouth kissing Justin C. Crandall's exposed uncircumcised penis during which Justin D. Crandall's entire face is visible.
- "20170116_232332.mp4": This video file depicts Justin D. Crandall forcing his exposed uncircumcised penis into [REDACTED] mouth. [REDACTED] is seated on the toilet in the bathroom of Justin D. Crandall's residence. [REDACTED] eyes were wide open and she appears to be in fear of her life. Justin D. Crandall spat on her face twice at two different points in the video file. Justin D. Crandall also choked [REDACTED] with his hand. [REDACTED] struggled to breath and opened her mouth. Justin D. Crandall said he wanted to "choke the life out of you..." Justin D. Crandall also called [REDACTED] "you little fucking twat." Justin D. Crandall, at one point, looked at the

camera and said, "Here's Charlie." Justin D. Crandall can also be overheard saying, "Daddy, help me." At the end of video file, Justin D. Crandall stroked his penis while saying [REDACTED] first name.

"20170206_233821.mp4":

This video file depicts [REDACTED] seated on the floor being covered with mayonnaise by Jessica L. Crandall using a large spoon. [REDACTED] was covered all over her body from head to toe with mayonnaise. Jessica L. Crandall forced the spoon near [REDACTED] mouth. Justin D. Crandall was filming the video file and got verbally excited when Jessica L. Crandall forced the mayonnaise near [REDACTED] vaginal area. Jessica L. Crandall can be overheard saying to [REDACTED] "...that's how you are going to bed." With one hand, Justin D. Crandall can be seen tying [REDACTED] hands together with a stretchy car style bungee cord while Jessica L. Crandall held up [REDACTED] back and propped her forward. Justin D. Crandall then used a long, thin wooden dowel to hit [REDACTED] in the face and her upper leg area near her vaginal area. [REDACTED] was seen shaking uncontrollably during the video file and is crying.

35. Additionally, Special Agent Vizvary employed an alternative method to bypass and defeat the password lock on the Subject Cellular Telephone. Employing this alternative method, Special Agent Vizvary successfully conducted a file system extraction of the Subject Cellular Telephone using a commercial software package available to law enforcement agencies known as Universal Forensic Extraction Device (UFED). In reviewing the results of the file system extraction of the Subject Cellular Telephone, Special Agent Vizvary advised that the file system extraction bypassed the password lock which gained access to a small portion of the Subject Cellular Telephone but only extracted a limited portion of the data and other files stored within the Subject Cellular Telephone. However, embedded within the extracted data and files, Special Agent Vizvary and your affiant located six (6) different video files in a folder entitled, "Whore training", constituting the sexual exploitation of [REDACTED] not previously observed on or extracted from the 16GB Miro SD card inserted in a media slot within the housing of the Subject Cellular Telephone. A sample of these video files, which are available for the Court's review upon request, are described below as follows:

"20170116_232332.mp4":

This video file depicts Justin D. Crandall forcibly pushing his exposed uncircumcised penis into [REDACTED] mouth during which [REDACTED] pushed Justin D. Crandall's

penis away from her. [REDACTED] was standing in a cluttered room crying and breathing heavily. While filming the video himself, Justin D. Crandall then spit on [REDACTED] face and called her pretty. Justin D. Crandall also struck [REDACTED] in the face with his hand. Justin D. Crandall also forced his fingers inside of [REDACTED] diaper and moved his fingers back and forth under her diaper near her vaginal area and most likely touched her vagina. Justin D. Crandall also choked [REDACTED]. During the video file, Justin D. Crandall can be overheard saying to [REDACTED] "...hi, Mommy" and "...little whore."

"20170116_231135.mp4":

This video file depicts [REDACTED] standing alone in the dark at Justin D. Crandall and Jessica L. Crandall's residence. While filming the video himself, Justin D. Crandall choked [REDACTED] several times with his hand. Justin D. Crandall also spat on [REDACTED] face and then wiped it off her face. [REDACTED] was observed crying and breathing heavily through the video file. [REDACTED] also appeared scared and upset. Justin D. Crandall can be overheard taunting [REDACTED] by saying [REDACTED] mother's first name and the following phrases: "so stinking cute", "help me, Mommy", and "she isn't gonna help you ever."

"20170123_191126.mp4":

This video file depicts [REDACTED] lying on bed in a diaper at Justin D. Crandall and Jessica L. Crandall's residence. [REDACTED] face was covered in tears as she stared directly at the camera. While filming the video himself, Justin D. Crandall can be overheard saying, "Mommy, [REDACTED] if you're reading this, I didn't make it." Justin D. Crandall then forcibly touched [REDACTED] chest and shook her body. Justin D. Crandall then looked directly at the camera and said, "...if you're reading this [REDACTED] I didn't make it." Justin D. Crandall then forced [REDACTED] to sit on her butt on the bed. Justin D. Crandall then pushed [REDACTED] back on the bed. [REDACTED] can be observed stiff as a board on the bed and staring directly at the camera. Justin D. Crandall can be overheard saying, "...don't fucking do it." Justin D. Crandall then forcibly pulled on [REDACTED] leg causing her to jump and move closer to his position on the bed at which time the video file ended.

36. On March 17, 2017, Justin D. Crandall and Jessica L. Crandall were indicted in United States District Court, Northern District of New York, by a Federal Grand Jury in Binghamton, New York, in connection with the captioned matter. After the Federal Grand Jury presentation, Justin D. Crandall and Jessica L. Crandall were charged with one (1) count of Title 18, United States Code, Section 2251(a)&(e) [Conspiracy to Sexually Exploit a Child], and five (5) counts of Title 18, United States Code, Section

2251(a)&(e) and 2(a) [Sexual Exploitation of a Child/Production of Child Pornography]. In addition to these charges, Justin D. Crandall was also charged with one (1) count of Title 18, United States Code, Section 2252A(a)(2)(A)&(b)(1) [Distribution of Child Pornography].

37. As of August 21, 2017, the FBI, Albany Field Division, Binghamton Resident Agency, has not been able to completely access all of the data and all files stored within the Subject Cellular Telephone that was used by Justin D. Crandall and Jessica L. Crandall to conspire and sexually exploit [REDACTED]. As demonstrated above in this affidavit, two different techniques to extract some data and some other information from the Subject Cellular Telephone resulted in locating different images and video files constituting the child sexual exploitation of [REDACTED], but failed to provide all chat logs, text messages, multimedia messages, Internet browsing history, downloaded and installed applications, e-mail messages, and all other file folders, etc. from the Subject Cellular Telephone. As a result, your affiant believes it is logical to infer should the Subject Cellular Telephone's entire file and data structure be extracted and accessible, additional images, video files, text messages, e-mail messages, etc. currently contained with the Subject Cellular Telephone but not instantly accessible to the FBI may contain additional evidence and information relative to the conspiracy and sexual exploitation of [REDACTED] by Justin D. Crandall and Jessica L. Crandall including additional photographs, video files, and text messages, and possibly inappropriate or otherwise illegal images and video files of Justin D. Crandall and Jessica L. Crandall's [REDACTED]

38. For instance, by Jessica L. Crandall's own admission to the New York State Police during her interview of February 13, 2017, Justin D. Crandall performed oral sexual contact on Jessica L. Crandall and then placed [REDACTED] head in her (Jessica L. Crandall) vaginal area for a period of approximately thirty seconds to one minute. Jessica L. Crandall advised she felt [REDACTED] nose touch her buttocks as Justin D. Crandall pushed [REDACTED] face into Jessica L. Crandall's vaginal area. Jessica L. Crandall advised that while [REDACTED] head was in her vaginal area, Justin D. Crandall informed her to look up and say "cheese" as he took a digital photograph using his cellular telephone, most likely the Subject Cellular Telephone, while [REDACTED] was situated in between Jessica L. Crandall's spread legs. To date, the

FBI and law enforcement have been unable to locate this particular image within the data and file structure of the Subject Cellular Telephone as previously partially unlocked, most likely because it is contained within a section of the Subject Cellular Telephone still inaccessible to the FBI. The FBI seeks to utilize different techniques not already tried or attempted in order to search the Subject Cellular Telephone for the items more particularly described in Attachment B. The FBI currently has reason to believe that a current technique(s) exist that will allow for extraction of password protected data and files from the Subject Cellular Telephone which were not able to be extracted during the previous search. For that reason application is made for this search warrant.

COMPUTERS, ELECTRONIC STORAGE, AND FORENSIC ANALYSIS

39. Your affiant has spoken with law enforcement investigators trained in computer and cellular telephone evidence recovery that have extensive knowledge about the operation of cellular telephones and computer systems including the correct procedures for the seizure and analysis of these systems. For the following reasons, your affiant submits there is probable cause to believe the information sought to be seized from the electronic media recovered will be stored on storage medium, or that the evidence thereof may be gained from a detailed forensic analysis of the media:

40. Searches and seizures of digital evidence from cellular telephones and computers commonly require agents and other law enforcement investigators to download or copy information from the cellular telephone, the computer, their components, and/or to seize most or all computer items to be processed later by a qualified computer expert or examiner in a laboratory setting or other controlled environment. This is almost always true because of the following reasons:

41. Cellular telephones and computer storage devices (like hard drives, diskettes, tapes, laser disks, magneto optical, and other storage related devices) can store the equivalent of millions of pages of information. When the user wants to conceal criminal evidence, he or she often stores this information in random order with deceptive file names. This requires searching authorities to examine all the stored data that is available in order to determine whether it is included in the search warrant that authorized the

search or not. As a result, this sorting process may take the examiner several days or even weeks and months, depending on the volume of data stored and its level of complexity.

42. Searching cellular telephones and computer systems for evidence is a highly technical process requiring expert skill and a controlled environment. The vast array of computer hardware and software available requires even computer experts to specialize in some systems and applications, so it is difficult to know before a search which expert should analyze the system and its corresponding data. The search of a cellular telephone or computer is an exacting scientific procedure that is designed to protect the integrity of the evidence and to recover even hidden, erased, compressed, password-protected, and/or encrypted files. Since computer or digital evidence is extremely vulnerable to tampering or destruction (which may be caused by malicious codes or normal activities of an operating system), the controlled environment of a forensic laboratory is essential to its accurate analysis.

43. Based on my knowledge, training, and experience, your affiant is aware that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, transferred, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost to the user. Even when files have been deleted, they can be recovered months or years later using specialized forensic tools. This is so because when a person “deletes” a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

44. Therefore, deleted files or remnants of deleted files may reside in free space or slack space—that is, in space located on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer’s operating system may also keep a record of deleted data or process in a “swap” or “recovery” file.

45. Apart from user-generated files, computer storage media—in particular, computers’ hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and more importantly, who has used it recently and in the past. This evidence can take the form of operating system configurations, artifacts from operating system or different application operation, file system data

structures, and the virtual memory “swap” or paging files. Computer users typically do not erase or delete this type of computer forensic evidence because special software is typically required for that task. However, it is technically possible to delete this information.

46. Similarly, files viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or “cache” located on the computer or cellular telephone. The browser often maintains a fixed amount of hard drive space devoted to these files, and the files are only overwritten as they are replaced with more recently viewed Internet pages or if a user takes steps to delete them.

47. Although some of the information called for by this search warrant might be found in the form of user-generated documents (such as word processor notes, photographic images, and video files), computer, smart phone style cellular telephones, and digital recording device (such as digital cameras and video cameras) storage media can contain other forms of electronic evidence as well:

47a. Forensic evidence of how the Subject Cellular Telephone were used, the purpose of its use, who used the Subject Cellular Telephone, and when, is called for by this search warrant. Data on the storage medium not currently associated with any file can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames, usernames, and passwords. Operating systems can record other information such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the dates and times the computer or cellular telephone was in use by the operator. Computer file systems can record information about the dates and times files were created and the sequence in which they were created.

47b. Forensic evidence on a computer or storage medium can also indicate who has used or controlled the computer or storage medium. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence or physical location. For example,

registry information, configuration files, user profiles, e-mail address books, "chats," instant messaging logs, photographs, and correspondence (and the data associated with the foregoing, such as file creation and last accessed dates and times) may in and of themselves be evidence of who used or controlled the computer, storage medium, or cellular telephone at a relevant time in question.

47c. A person with appropriate familiarity with how a computer or cellular telephone works can, after examining this forensic evidence in its proper context, draw logical conclusions about how computers and/or cellular telephones were used, the purpose of their use, who used them, and when.

47d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance with particularity a description of the records to be sought, evidence of this type often is not always data that can be merely reviewed by a review team and passed along to the case agents and investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand the nature of the evidence described in Attachment B also falls within the scope of the search warrant.

47e. Searching storage media for the evidence described in the attachment may require a range of data analysis techniques. It is possible that the storage media will contain files and information that are not called for by the search warrant. In rare cases, when circumstances permit, it is possible to conduct carefully targeted searches that can locate evidence without requiring a time-consuming manual search through unrelated materials that may be commingled with criminal evidence. For example, it is possible, though rare, for a storage medium to be organized in a way where the location of all things called for by the search warrant is immediately apparent. In most cases, however, such techniques may not yield the evidence described in the search warrant. For example, information regarding user attribution or Internet use is located in various operating system log files that are not easily located or reviewed. As explained above, because the search warrant calls for records of how the Subject Cellular Telephone has been used, what it has been used for, and who has used it, it is exceedingly likely that it will be necessary to

thoroughly search storage media to obtain evidence including evidence that is not neatly organized into files or documents. Just as a search of a premises for physical objects requires searching the entire premises for those objects that are described by a search warrant, a search of the Subject Cellular Telephone for the things described in this search warrant will likely require a search among the data stored in storage media for the things (including electronic data) called for by this search warrant. Additionally, it is possible that files have been deleted or edited, but that remnants of older versions are in unallocated space or slack space. This, too, makes it exceedingly likely that in this particular case it will be necessary to use more thorough techniques.

SEARCH METHODOLOGY TO BE EMPLOYED

48. The search procedure of electronic and digital data contained in cellular telephones, computer hardware and software, and/or memory storage devices may include the following techniques (the following is a non-exclusive list, as other search procedures may be used):

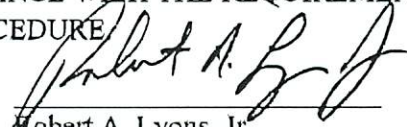
- a. examination of all of the data contained in such cellular telephone or computer hardware, computer software, or memory storage devices to view the data and determine whether that data falls within the items to be seized as set forth herein;
- b. searching for and attempting to recover any deleted, hidden, or encrypted data to determine whether that data falls within the list of items to be seized as set forth herein (any data that is encrypted and unreadable will not be returned unless law enforcement personnel have determined that the data is not (1) an instrumentality of the offenses, (2) a fruit of the criminal activity, (3) contraband, (4) otherwise unlawfully possessed, or (5) evidence of the offenses specified above);
- c. surveying various file directories and the individual files they contain;
- d. opening files in order to determine their contents and scanning storage areas;
- e. performing key word searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are likely to appear in the evidence described in Attachments B; and

- f. performing any other data analysis technique that may be necessary to locate and retrieve the evidence described in Attachment B.


CONCLUSION

49. Based on the aforementioned information, your affiant respectfully submits that there is probable cause to believe that child pornography (specifically, sexually explicit images of R.A. and other minors known and unknown, were produced, received, distributed and/or possessed by Justin D. Crandall and Jessica L. Crandall, in violation of Title 18, United States Code, Sections 2251, 2252 and 2252A) as well as other personally identifying information necessary to confirm the owner and operator of the Subject Cellular Telephone, and other relevant evidence tying Justin D. Crandall and Jessica L. Crandall to R.A. and her sexual and physical exploitation will be located within the Subject Cellular Telephone that is the subject of this search warrant. Therefore, based upon the information contained in this affidavit, your affiant requests this Court issue the attached search warrant and application authorizing the FBI to utilize different techniques not already tried or attempted in order to search the Subject Cellular Telephone for the items more particularly described in Attachment B. The FBI currently has reason to believe that a current technique(s) exist that will allow for extraction of password protected data and files from the Subject Cellular Telephone which were not able to be extracted during the previous search. For that reason application is made for this search warrant.

ATTESTED TO BY THE APPLICANT IN ACCORDANCE WITH THE REQUIREMENTS OF RULE 4.1 OF THE FEDERAL RULES OF CRIMINAL PROCEDURE


Robert A. Lyons, Jr.
Special Agent
Federal Bureau of Investigation

Sworn to before me this 24th day
of August 2017.


HONORABLE THERESE WILEY DANCKS
UNITED STATES MAGISTRATE JUDGE
NORTHERN DISTRICT OF NEW YORK

ATTACHMENT A
DESCRIPTION OF THE ELECTRONIC ITEMS TO BE SEARCHED

The Subject Cellular Telephone is currently secured at the Office of the FBI, Albany Field Division, Syracuse Resident Agency, business address 250 South Clinton Street, Syracuse, New York 13202, and is fully identified and described below as follows:

The Subject Cellular Telephone:

1. One (1) black colored Samsung Cellular Telephone, Model #: SM-S120VL(GP), FCC ID #: A3LSMS120VL, Serial #: GPSAS120VCB, IMEI #: 359259071509110, Made in Vietnam, with one (1) camouflage and black colored plastic case.

ATTACHMENT B
LIST OF ITEMS TO BE SEIZED AND SEARCHED FROM THE SUBJECT CELLULAR
TELEPHONE IN ATTACHMENT A

Items and information that constitute fruits, evidence and instrumentalities of violations of Title 18, United States Code, Sections 2251 (sexual exploitation of children, and the attempt and conspiracy to commit that offense), and 2252/2252A (receipt, distribution, and/or possession of child pornography, and the attempt to commit said offenses) including:

Computers, Electronic Media, and Internet Records

1. The authorization includes the search of electronic data to include deleted data, remnant data and slack space. The search of the Subject Cellular Telephone and electronic media, and the seizure of information contained therein will be conducted in accordance with the affidavit submitted in support of this search warrant.
2. Documentation that explains or illustrates the configuration or use of Subject Cellular Telephone.
3. Cellular telephone passwords, computer passwords, and programs, or data, that can be used or are designed to be used to restrict access to, or to facilitate concealment of, any hardware, software, computer related documentation, or electronic data records.
4. Any cellular telephone, computer, or electronic records, documents and materials referencing or relating to the above described offenses, as well as their drafts or modifications, in whatever form stored on the Subject Cellular Telephone.
5. Any electronic information or data, stored in any form, which has been used or prepared for use either for periodic or random backup (whether deliberate, inadvertent, or automatically or manually initiated), of the Subject Cellular Telephone.
6. Records of personal and business activities relating to the use, operation, and ownership of the Subject Cellular Telephone.
7. Records of address or identifying information for the target of the investigation and any personal or business contacts or associates of his, (however and wherever written, stored or maintained), including contact lists, buddy lists, email lists, ICQ addresses, IRC names (a.k.a., "Nics"), user ID's, eID's (electronic ID numbers) and passwords stored on the Subject Cellular Telephone.
8. Personal and business documents, records, monthly statements, payment and billing history, and telecommunications carrier invoices regarding the ownership and/or possession stored on and within the Subject Cellular Telephone.
9. Records and evidence identifying who the particular user or users were who possessed, distributed, or produced any child pornography found on Subject Cellular Telephone or electronic media (evidence of attribution), and how Subject Cellular Telephone possessed, distributed or produced the child pornography including but not limited to the images and video files of [REDACTED]

Materials Relating to Child Erotica and Depictions of Minors

10. Visual depictions of minors, including but not limited to, the sexually explicit images and video files of any and all minors to include [REDACTED]
11. Correspondence, chats, chat logs, e-mail messages, text messages, and other text documents describing or relating to sexually explicit conduct with children to include [REDACTED] as well as any fantasy writings regarding, describing, or showing a sexual desire and interest in minor children.
12. Address books, names, and lists of names and addresses of minors visually depicted while engaged in sexually explicit conduct, as defined in Title 18, United States Code, Section 2256(2).
13. Child erotica, including photographs and video files of children that are not sexually explicit, drawings, sketches, fantasy writings, notes, and sexual aids.
14. Internet history including evidence of visits to websites that offer visual depictions of minors engaged in sexually explicit conduct as defined in Title 18, United States Code, Section 2256.
15. Documents, photographs, and digital video files relating to the receipt, distribution, transmission, advertisement, production, and possession of child pornography or child erotica, including evidence regarding the source of those image and video files, including dates and manner of receipt/download, and evidence regarding whether those image and video files were transported or distributed using a means and facility of or in and affecting interstate and foreign commerce, including dates and manner of transportation/distribution.
16. Any and all records or communications evidencing intent, conspiracy, and/or plans to engage in sexually explicit conduct with [REDACTED] discussions between [REDACTED] and Justin Crandall regarding [REDACTED], other unknown subjects, and any other minor children.
17. Any notes, writings, or other evidence that would assist law enforcement in identifying additional victims of sexual exploitation, witnesses thereto, or other subjects that may have assisted, conspired, or agreed to participate in the sexual exploitation of [REDACTED] by Justin D. Crandall and Jessica L. Crandall as well as any other individuals.